计算机工程与应用 2007 43 (1期): 148 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

基于密钥服务器的IEEE 802.11i密钥更新方案

周贤伟, 白浩瀚, 覃伯平

北京科技大学信息工程学院

收稿日期 2006-5-10 修回日期 网络版发布日期 接受日期

摘要 随着WLAN的广泛应用，无线安全越来越受到人们关注，密钥管理作为安全系统的实现基础亟待解决。针对IEEE 802.11i标准为产生新的对等密钥PTK，STA与AP之间需要重新进行四步握手协议而加重STA开销的问题，提出一种基于密钥服务器的密钥更新方案（KSRS）。该方案对802.11i的密钥层次结构进行修改，增加了密钥更新层，可达到集中密钥更新的目的；结合STA的漫游特性，借鉴集中式密钥管理思想，引入可信实体KS来分发并更新密钥，可提供灵活的密钥管理操作。经性能分析，该方案的开销较小，能更加适应STA的移动性。

关键词 无线局域网,强安全网络,扩展认证协议,消息完整性码

分类号

A Key Server based Re-keying Scheme of IEEE 802.11i

,,

北京科技大学信息工程学院

Abstract

With the wide application of WLAN, wireless security has become a serious concern for an increasing number of people. As the basis of implementing a security system, key management is a problem to be solved urgently. To derivate a new Pairwise Transient Key (PTK), 4-Way Handshake needs to be carried out repeatedly between STA and AP, which worsens the overheads of STA. Aiming at this problem, a Key Server based Re-keying Scheme (KSRS) was proposed. This scheme adds a new level called Re-keying Level to the key hierarchy of 802.11i, which can implement centralized re-keying. Considering roaming character of STA and referring the centralized key management approach, this scheme uses an authentic entity called Key Server (KS) to distribute and refresh the keys, which can provide flexible operations for key management. A performance analysis on this scheme shows that it has lower overheads; thus it can be more suitable for mobility of STA.

Key words WLAN RSN EAP MIC

DOI:

通讯作者 白浩瀚 hhbai haohanb@126.com

扩展功能

本文信息

- Supporting info
- PDF(0KB)
- [HTML全文](0KB)
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 复制索引
- Email Alert
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“无线局域网,强安全网络,扩展认证协议,消息完整性码”的 相关文章
- 本文作者相关文章
  - 周贤伟
  - 白浩瀚
  - 覃伯平